Cyber Security Awareness

State of Alabama
Information Services Division (ISD)

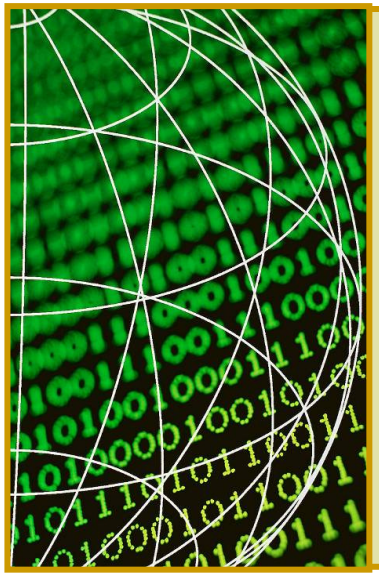
Purpose

- Ensure all employees receive timely cyber security awareness and training, appropriate to their roles and responsibilities, to increase awareness of information security risks, increase technical competence, and ensure compliance with information security policies and standards.
- Ensure all users are exposed to basic information system security awareness materials before authorizing access to the system and at least annually thereafter.

— State IT Policy 610-01

Cyber Security Goals

- Number 1 - Protect the data
- Number 2 - Protect the systems that store and process the data



There are many threats to data and systems and many layers of control.

System users need to be aware of both the threats and the controls.

Applications Under Attack

- "Today, over 70% of attacks against a company's network come at the 'Application Layer,' not the Network or System Layer."

  — Gartner Group

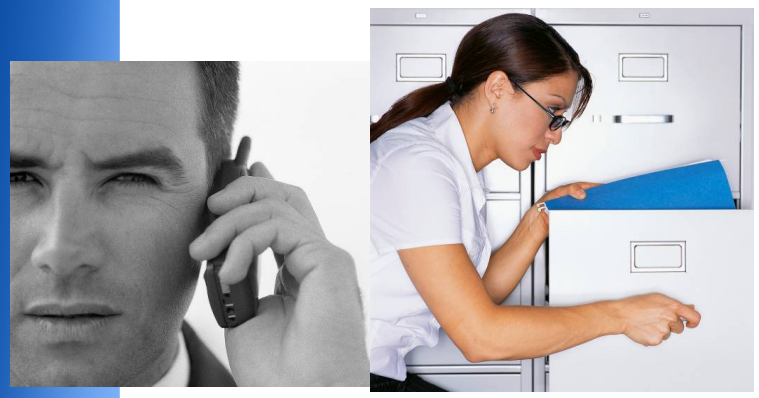
- Operating Systems
  - Windows Services
  - Internet Explorer
  - Microsoft Office
  - Mac OS X
- Cross-Platform Applications
  - Web Applications
  - Database Software
  - P2P File Sharing
  - Instant Messaging
  - Media Players
  - Backup Software

Attack Vectors

- E-mail / Attachments
- Web Access and Downloads
- Thumb Drives
- Removable Media
- Wireless Communication Devices (PDA, Cell Phone)
- Intelligent Peripherals (printers, faxes, etc.)
- Viruses/Worms/Malware
- Social Engineering

Social Engineering Threat

- Social Engineering Techniques
  - Phishing
  - Spam / Gimmes
  - Phone Calls / Pretexting
  - Trash / Dumpster Diving



"People, by nature, are unpredictable and susceptible to manipulation and persuasion. Studies show that humans have certain behavioral tendencies that can be exploited with careful manipulation. Many of the most-damaging security penetrations are, and will continue to be, due to social engineering, not electronic hacking or cracking. …

"We believe social engineering is the single greatest security risk in the decade ahead. "

— Gartner Group

Security Policies & Standards

- http://isd.alabama.gov

Network/System Access

- Users are accountable for policy-compliant use of systems
- Users must be authorized to access network or systems
- Access to data is based on:
  - Sensitivity of the information
  - User's need to know

— State IT Policy 620-01

Activity Monitoring

- Authorized access does not imply a user's right to privacy.
- System and network activities may be logged, recorded, and reviewed by management or other authorized personnel.

— State IT Policy 620-01

Why Are Passwords Required?

- Authentication
- Access Control
- Accountability
- Data Integrity
- Prevention of unauthorized (intentional or unintentional) disclosure, destruction, or modification of all computer or network hardware, software, data, and documentation

— State IT Policy 620-03

Passwords

- Never share passwords
- Never write passwords down
- Change passwords at least every 90 days
- Passwords must be at least 8 characters in length
- Combine upper/lower case, numeric, and special characters

How Long Does It Take to Hack a Password?

Length of Password	Using			
	26 Characters (lower case a-z) ***password***	**52 Characters** (mixed upper A-Z and lower a-z) ***PassWord***	**62 Characters** (mixed upper, lower, and numbers) ***Pass12Word***	**96 Characters** (mixed upper, lower, numbers, and special) ***Pass1#2$Word***
2	Instantly	Instantly	Instantly	Instantly
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	<2 seconds	<9 seconds
5	Instantly	38 seconds	<2 minutes	<14 minutes
6	30 seconds	33 minutes	<2 hours	22 hours
7	13 minutes	28 hours	4 days	87 days
8	<6 hours	62 days	253 days	23 years
9	6 days	9 years	* * *	* * *
10	163 days	* * *	* * *	* * *

Based on Class D attacking computer: fast dual-processor PC (10,000,000 attempts per second)

Internet Access

- Access to the Internet is provided as a business and informational resource to support and enhance the capability of Internet users to carry out their job responsibilities
- The State reserves the right to access, monitor, or disclose all Internet activity as required in the course of monitoring, auditing, or responding to legal processes or investigative procedures.

— State IT Policy 630-02

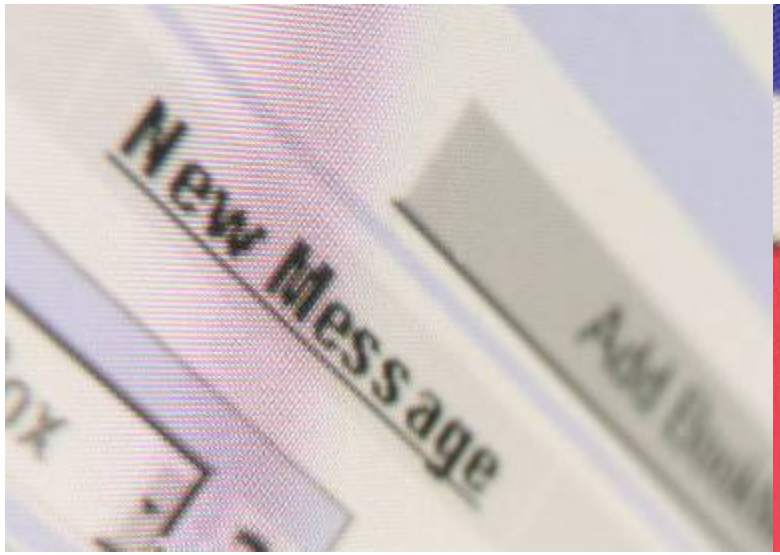
Prohibited Uses

- Games and on-line gambling
- Activities in support of private business enterprises
- Unauthorized reproduction of copyrighted material

— State IT Policy 630-05

E-Mail Use

- Used for business purposes and occasional personal use
- No confidentiality; subject to monitoring
- Handle attachments with caution; common source of malware



— State IT Policy 630-03

Instant Messenger (IM) Programs

- Use only approved IM clients and settings
- For business communications only, when no practical alternative exists
- Limited to text messages only; IM file transfers are blocked
- NOT to be used to communicate sensitive or confidential information
- No confidentiality; IM communications subject to monitoring

— State IT Policy 630-04

Viruses and Malware

- Hardware, software, or firmware intentionally introduced in a computer system for an unauthorized purpose
  - It is designed with a malicious intent to deny, destroy, modify, or impede systems configuration, programs, data files, or routines
- How viruses and malware are transmitted
  - Attachments to e-mail or instant message
  - Internet downloads
  - Portable or bootable storage (CD, diskette, USB device)
  - Malicious Web sites

Malware Prevention

- Scan portable storage media (diskettes, CDs, USB drives, etc.) before files residing on the media are accessed
- Update AV software with the most current virus definitions; use automatic updates whenever possible

Malware Incident

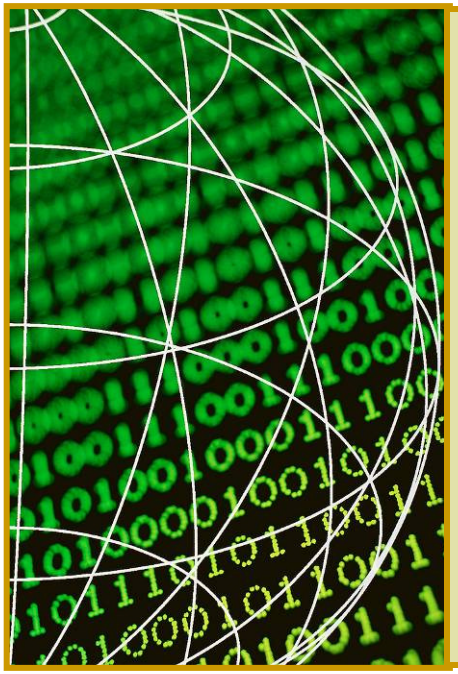
- Disconnect from the network IMMEDIATELY!
- Contact the Help Desk, System Administrator, or ISO
- Scan and disinfect system using approved anti-virus software
- Scan all portable storage devices and media
- Mitigate vulnerabilities exploited by malware
- Test system to confirm normal operation
- Return system to service

Other Cyber Security Incidents

- Unauthorized access to a network, system, and/or data
- Repeated attempts at unauthorized access
- System changes not authorized by nor known to the system owner
- Denial of Service attack or other disruptions to service
- Evidence of tampering with, removal of, or loss of data
- Web site defacement
- Social engineering incidents
- Theft of, or non-accidental physical damage to, information systems
- Evidence of inappropriate use or other noncompliance with policies or standards

Incident Response Assistance

- Help Desk
- Cyber Security Incident Response Team (CSIRT)
- Information Security Officer
- IT Manager
- Law Enforcement



Report Incidents To:

Help Desk
(334-242-2222)

Information Security Officer

IT Manager

What Must Be Reported?

- Systems or sites involved
- Incident description
- Date, time, and method of incident discovery
- Severity and impact of the incident
- Classification of potentially compromised system and/or data
- Actions already taken to secure or restore the system and/or data

For Further Information…

Lee Styres

Chief Information Security Officer

Information Services Division, Dept. of Finance

334-242-3044

lee.styres@isd.alabama.gov